令和５（２０２３）年度　卒業研究報告書概要

課程，学籍番号，氏名	課程：電気・電子情報工学課程，学籍番号：B223233，氏名：工藤　典佑
工学分野名：情報通信システム	指導教員名：市川　周一

題　　目：和　天文画像と LFSR による乱数生成手法の検討

（英　Investigation of Random Number Generation Method Using Astronomical Images and LFSR）

Abstract

Random number generation plays a crucial role in various fields, particularly in security technology, cryptography, and simulation applications. This study introduces a practically unpredictable random number generator (URNG; Unpredictable Random Number Generator) using astronomical images as an entropy source. Multiple methods for processing celestial images were examined and verified. The generated random numbers were then evaluated using the DIEHARD test. Notably, all 18 methods passed the DIEHARD test by using galaxy images. On the other hand, with the extragalactic images, two of the 18 methods failed the Binary Rank (31x31) and the Binary Rank (32x32) test, when the integer part of pixel data was used.

概　　要

乱数生成は，特定の分野，特にセキュリティ技術・暗号化技術・シミュレーション用途などにおいて非常に重要である．当研究室では，プロセッサに LFSR (Linear Feedback Shift Register)を組み込むことにより，実質的に予測不能な乱数生成器 (URNG; Unpredictable Random Number Generator)が実現可能であることを示した．正岡らの研究では，サンプリング間隔の揺らぎが乱数のエントロピー源となっていたが，LFSR をハードウェアとして実装する必要があった．しかし，何らかのエントロピー源を基にサンプリング間隔を変動させれば，ソフトウェアで LFSR をシミュレートすることにより URNG を構成することができる．

市川は，画像情報をエントロピー源とした URNG を提案した．LFSR のサンプリング間隔を画像情報で変動させることにより URN (Unpredictable Random Number)を生成した結果，画像の最下位ビットで揺らぎを与えた場合に，DIEHARD テストに合格することを示した．市川の研究では，SIDBA の標準画像が用いられており，それ以外の画像では乱数品質が検証されていない．また，民生用のカメラでは，ノイズ除去等の画像処理や絵作りが行われており，自然由来のエントロピーとは異なる可能性がある．そこで本研究では，予測が困難な自然対象の観測データとして SPITZER の天文画像を採用した．

本研究で使用した天文画像は fits ファイルであり，銀河系・銀河系外及び MIPS・IRAC の装置で観測された 4 枚を使用した．天文画像の 1 ピクセルは整数部最大 4 桁，小数部最大 6 桁で構成されている．この値の取得に関していくつかの手法を提案し，各手法の妥当性の検証及び乱数の生成，乱数品質の評価を行った．その後，算出された値を 2 進数変換し，揺らぎとして用いた．この時，画像のピクセル値は一次元配列に格納し，配列への格納順で循環的に使用した．乱数品質の評価には DIEHARD テストを使用した．

結果として，銀河系の画像では，18 種全てのテストに合格した．一方で銀河系外の画像では整数部を取得する手法において 18 種のうち 2 種のテストに不合格であり，Binary Rank(31x31) や Binary Rank (32x32)のテストに FAIL した．よって，入力データ量が大きく情報エントロピーの高い銀河系画像では乱数品質が高いことが示された．また，観測装置による乱数品質の差はみられない．全ての画像において共通して，小数部を取得する手法は整数部を取得する手法と比較すると乱数品質が高い．小数部を取得するいくつかの手法では乱数品質に大きな差が観測されなかった．よって，小数部の少ない桁数を取得する手法が乱数生成において推奨される．本研究では，数枚の天体画像しか用いられていないため，より多くの天体画像を用いて実験し，条件を細分化しながら高品質な乱数を実現する手法を見出すことが今後の課題である．

発表する際の課程を記入　　電気・電子情報工学　課程　　発表番号　47

（学籍が他課程所属の学生も発表する課程を記入すること）